AMPLIACIÓN DE MATEMÁTICAS

CLASIFICACIÓN DE GRUPOS FINITOS.

Vamos a ver una clasificación de los grupos finitos. Va a ser un poco superficial, pero nos dará una idea de como puede ser usada en algunas aplicaciones. Desde el cálculo en paralelo a la descripción de los cuerpos finitos.

Comenzaremos con los grupos cíclicos. Seguiremos con los grupos abelianos finitos y algo diremos de los no abelianos.

GRUPOS CÍCLICOS.

Ejemplos 1. $(\mathbb{Z}_n, +)$ *y* $(\mathbb{Z}, +)$ *son ejemplos de grupos cíclicos ya que*

$$< [1]_n >= \mathbb{Z}_n \qquad y \qquad < 1 >= \mathbb{Z}.$$

Teorema 1. **A:** *Sea* $(\mathbb{G}, *)$ *un grupo cíclico finito de orden* n*, entonces* $(\mathbb{G}, *)$ *es isomorfo a* $(\mathbb{Z}_n, +)$.

B: *Sea* $(\mathbb{G}, *)$ *un grupo cíclico infinito, entonces* $(\mathbb{G}, *)$ *es isomorfo a* $(\mathbb{Z}, +)$.

Demostración:

A: Si $g \in \mathbb{G}$ es un generador de $\mathbb{G}$ y $|\mathbb{G}| = n$, entonces

$$\mathbb{G} = \{\ g, g^2, ..., g^{n-1}, g^n = e\ \}.$$

Se considera la aplicación:

$$\begin{array}{rccccc} T & : & (\mathbb{Z}_n, +) & \to & (\mathbb{G}, *) & \\ & & [j] & \to & T([j]) & = & g^j. \end{array}$$

T claramente está bien definida y es una biyección. Veamos que es un homomorfismo y por tanto un isomorfismo.

$T([j] + [i]) = T([j + i]) = g^{j+i} = g^j * g^i = T([j]) * T([i])$.

(Si $j + i = n + r > n$, entonces

$$T([j] + [i]) = T([r]) = g^n * g^r = g^{n+r}$$
$$= g^{j+i} = g^j * g^i = T([j]) * T([i])\ \ )\ \square$$

B: Se considera la aplicación:

$$\begin{array}{rcccl} T & : & (\mathbb{Z},+) & \to & (\mathbb{G},*) =< g >= \{g^k \,:\, k \in \mathbb{Z}\} \\ & & n & \to & T(n) \qquad\qquad = \quad g^n. \end{array}$$

T claramente es una biyección y un homorfismo □

Corolario 1. *Todo grupo cíclico es abeliano.*

Demostración: Dado que es isomorfo a $(\mathbb{Z}_n,+)$ o $(\mathbb{Z},+)$ □

Corolario 2. *El grupo* $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+)$ *es cíclico si y solo si*

$$m.c.d.(m_1,m_2) = 1.$$

En este caso $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+)$ *es isomorfo a* $(\mathbb{Z}_{m_1\times m_2},+)$.

Demostración:

- Ya vimos, con la ayuda del Teorema Chino del Resto, que si $m.c.d.(m_1,m_2) = 1$, entonces la aplicación

$$\begin{array}{rcccl} T & : & (\mathbb{Z}_{m_1\times m_2},+) & \to & (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+) \\ & & [n] & \to & T([n]) \qquad = \quad ([n]_{m_1},[n]_{m_2}) \end{array}$$

  es un homomorfismo biyectivo, por tanto un isomorfismo. Lo cual nos dice también que $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+)$ es cíclico.
- Ahora, si $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+)$ es cíclico, por el Teorema anterior, tiene que ser isomorfo a $(\mathbb{Z}_{m_1\times m_2},+)$.

  Por otro lado si $m.c.d.(m_1,m_2) = d > 1$, entonces $m_1 = dk_1$, $m_2 = dk_2$ y $dk_1k_2 < m_1m_2$. Ahora para todo $(n,m) \in (\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+)$ se tiene que

$$(n,m) + (n,m) + ...{}_{dk_1k_2-\text{veces}}.., +(n+m) = (1,1).$$

  Luego ningún elemento de $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},+)$ puede ser un generador. Llegamos a contradicción. Así, $m.c.d.(m_1,m_2) = 1$ □

Ejemplo 1. $(\mathbb{Z}_{60},+)$ *es un grupo cíclico y es isomorfo a* $(\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5,+)$. *Sin embargo* $(\mathbb{Z}_6 \times \mathbb{Z}_{10},+)$ *es un grupo de orden* 60 *que no es cíclico y que no es isomorfo a los anteriores.*

En general se tiene que

Corolario 3. *Si $n \in \mathbb{N}\backslash\{0\}$ de modo que tiene una descomposición en potencias de primos distintos*

$$n = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}$$

entonces la aplicación

$$\begin{array}{rcccl} T & : & (\mathbb{Z}_n, +) & \to & (\bigoplus_{i=1}^k \mathbb{Z}_{p_i^{r_i}}, +) \\ & & [m] & \to & T([m]) = ([m]_{p_1^{r_1}}, ..., [m]_{p_k^{r_k}}) \end{array}$$

es un isomorfismo de grupos.

Observación 1.

- *La descomposición anterior vimos que servía para hacer "operaciones rápidas" (relacionado con la computación en paralelo).*
- *Calcular ordenes de elementos $m \in (\mathbb{Z}_n, +)$ es equivalente a calcular el orden de $T(m) \in (\bigoplus_{i=1}^k \mathbb{Z}_{p_i^{r_i}}, +)$.*
- *El ejemplo de arriba, $(\mathbb{Z}_6 \times \mathbb{Z}_{10}, +)$, de un producto que no es cíclico nos apunta en la dirección de como son los grupos abelianos **no** cíclicos.*

A continuación veremos como son los grupos abelianos no cíclicos.

GRUPOS ABELIANOS NO CÍCLICOS. Se puede probar, pero queda fuera de nuestras posibilidades, una extensión de los resultados anteriores en el caso de grupos finitos abelianos.

Teorema 2. *(**Principal de grupos finitos abelianos**). Cada grupo **finito abeliano** es isomorfo a una suma directa de grupos del tipo $(\mathbb{Z}_{p^r}, +)$ con p primo.*

Más concretamente, reordenando el enunciado anterior, se puede probar que:

Teorema 3. *Sea $(\mathbb{G}, *)$ un **grupo abeliano, finito y no cíclico**. Entonces existen números naturales $d_1, d_2, ..., d_s$ de modo que $d_1 > 1$, $d_i | d_{i+1}$ para $i = 1, 2, ..., s-1$ y además*

$$\mathbb{G} \qquad \text{es isomorfo a} \qquad (\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times .... \times \mathbb{Z}_{d_s}, +)$$

*Los números $d_1, d_2, ..., d_s$ están unívocamente determinados por $\mathbb{G}$ y se les llamas **divisores elementales** del grupo.*

Observación 2. *Si $d_i | d_{i+1}$, entonces $(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times .... \times \mathbb{Z}_{d_s}, +)$ no puede ser cíclico.*

El teorema anterior lo utilizaremos más adelante para probar que los grupos multiplicativos de los cuerpos finitos son todos cíclicos.

Ejemplo 2. *Queremos encontrar todos los grupos* ***abelianos*** *de orden* 100.

El orden 100 puede descomponerse en potencias de primos (Teorema Fundamental de la Aritmética).

$$100 = 2^2 \times 5^2.$$

Ahora, ésto nos permite hacer otras descomposiciones del tipo del teorema anterior.

- Si $s = 1$, $(\mathbb{Z}_{100}, +)$ es el único grupo cíclico de orden 100 (salvo isomorfismo; por ejemplo es isomorfo a $(\mathbb{Z}_4 \times \mathbb{Z}_{25}, +)$.
- Si $s = 2$ podemos escribir
  - $100 = 2 \times 50$, lo que nos da el grupo $(\mathbb{Z}_2 \times \mathbb{Z}_{50}, +)$.
  - $100 = 5 \times 20$, lo que nos da el grupo $(\mathbb{Z}_5 \times \mathbb{Z}_{20}, +)$.
  - $100 = 10 \times 10$, lo que nos da el grupo $(\mathbb{Z}_{10} \times \mathbb{Z}_{10}, +)$.
- Para $s = 3$ no podemos seguir descomponiendo 100. Observemos que

  $$(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}, +) \qquad \text{es isomorfo a} \qquad (\mathbb{Z}_2 \times \mathbb{Z}_{50}, +).$$

  O que

  $$(\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5, +) \qquad \text{es isomorfo a} \qquad (\mathbb{Z}_5 \times \mathbb{Z}_{20}, +).$$

Ejemplo 3. *Si p es primo $(\mathbb{Z}_p, +)$ es un grupo cíclico. Sin embargo, $(\mathbb{Z}_{p^2}, +)$ es cíclico, pero $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$ no lo es.*

Ejemplo 4. *Vamos a hacer la lista completa de los grupos abelianos de orden menor o igual que* 15 *(salvo isomorfismo).*

- Los grupos $(\mathbb{Z}_1,+),(\mathbb{Z}_2,+),....,(\mathbb{Z}_{14},+)$ y $(\mathbb{Z}_{15},+)$ son todos cíclicos. Además los grupos de ordenes primos: $2,3,5,7,11$ y 13 son todos cíclicos y ya están en la lista anterior.
- De orden 4. Como $4=2\times 2$, tenemos el grupo no cíclico $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$.
- De orden 6. Como $6=2\times 3$, **no** tenemos un grupo nuevo ya que $(\mathbb{Z}_2\times\mathbb{Z}_3,+)$ es cíclico.
- De orden 8. Como $8=2\times 4$ y $8=2\times 2\times 2$, tenemos los grupos no cíclico $(\mathbb{Z}_2\times\mathbb{Z}_4,+)$ y $(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,+)$.
- De orden 9. Como $9=3\times 3$, tenemos el grupo no cíclico $(\mathbb{Z}_3\times\mathbb{Z}_3,+)$.
- De orden 10. Como $10=2\times 5$, **no** tenemos un grupo nuevo ya que $(\mathbb{Z}_2\times\mathbb{Z}_5,+)$ es cíclico.
- De orden 12. Como $12=2\times 6$, tenemos el grupo no cíclico $(\mathbb{Z}_2\times\mathbb{Z}_6,+)$.
- De orden 14. Como $14=2\times 7$, **no** tenemos un grupo nuevo ya que $(\mathbb{Z}_2\times\mathbb{Z}_7,+)$ es cíclico.
- De orden 15. Como $15=3\times 5$, **no** tenemos un grupo nuevo ya que $(\mathbb{Z}_3\times\mathbb{Z}_5,+)$ es cíclico.

Hay en total 15 **grupos cíclicos** y 5 **grupos abelianos no cíclicos** de orden menor o igual a 15.

GRUPOS NO ABELIANOS. La clasificación de los grupos finitos no abelianos es mucho más compleja y queda fuera de nuestro alcance. Decir solamente que la clasificación completa fué un problema abierto hasta no hace mucho.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

Email address: Cesar_Ruiz@mat.ucm.es